(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112652097 A
(43)申请公布日 2021.04.13

(21)申请号 202011486741.7

(22)申请日 2020.12.16

(71)申请人 浙江大学
地址 310058 浙江省杭州市西湖区余杭塘路866号

(72)发明人 孙怡琳 史治国 李颖 李传武 陈积明

(74)专利代理机构 杭州求是专利事务所有限公司 33200
代理人 刘静

(51)Int.Cl.
G07C 9/00(2020.01)

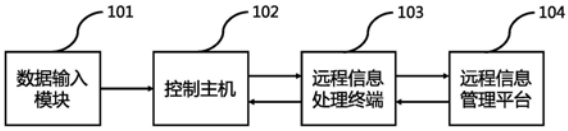
权利要求书3页 说明书6页 附图3页

(54)发明名称

商用车远程防盗系统及其工作方法

(57)摘要

本发明公开了一种商用车远程防盗系统及其工作方法，该系统主要由数据输入模块、控制主机、远程信息处理终端和远程信息管理平台构成。针对CAN通信时信息泄漏、数据修改、重放攻击等问题，本发明在传统的CAN数据传输上增加加密/解密机制，并向原始数据中融入计数器值和消息认证码，本发明在网络良好状态下将授权信息从远程信息管理平台实时下发至远程信息处理终端存储，控制主机上电时基于CAN通信获取远程信息处理终端存储的授权信息，防止因网络问题导致信息预置失败而影响系统工作，本发明使用远程信息管理平台对挂车和司机信息可视化管理，实现下发控制命令和更新授权信息的功能，从而帮助物流公司实现远程车队管理及挂车防盗工作。



CN 112652097 A

1.一种商用车远程防盗系统,其特征在于,包括数据输入模块、控制主机、远程信息处理终端和远程信息管理平台;所述数据输入模块、控制主机和远程信息处理终端设置在商用车上;所述数据输入模块和控制主机在商用车上电时启动,所述远程信息处理终端通过储能单元供电长时间运行;

所述数据输入模块包括身份识别器和附属控制器,所述身份识别器用于识别司机专属身份卡信息,所述附属控制器用于将司机身份卡信息加密后传输至控制主机;

所述控制主机包括存储模块和解密模块,接收所述数据输入模块传输来的信息,通过解密模块对信息进行解密得到司机身份卡信息,与存储模块中预置的授权信息进行匹配验证,授权信息包括有效司机身份卡信息和授权时间段,验证通过后执行解锁工作,并将商用车当前上锁/解锁状态传输至远程信息处理终端;接收所述远程信息处理终端传输的控制指令,执行相应的解锁/上锁工作,并将商用车当前上锁/解锁状态传输至远程信息处理终端;在上电时,向远程信息处理终端发送授权信息更新请求,接收远程信息处理终端传输的最新授权信息,通过解密模块进行解密得到最新的有效司机身份卡信息和授权时间段,更新存储模块中预置授权信息;

所述远程信息处理终端包括存储模块和加密模块,用于将所述控制主机传输的商用车当前上锁/解锁状态转发至远程信息管理平台;将远程信息管理平台下发的控制指令转发至控制主机,将远程信息管理平台下发的授权信息存储在其存储模块;接收控制主机发送的授权信息更新请求后,将存储模块中的授权信息通过加密模块加密后发送至控制主机;

所述远程信息管理平台用于可视化当前商用车状态以及司机的信息,管理员可通过所述远程信息管理平台下发上锁/解锁控制指令及更新授权信息。

2.根据权利要求1所述的一种商用车远程防盗系统,其特征在于,所述加密机制具体如下:

A1:将拼接了计数器值的原始数据和密钥作为认证算法输入,计算获取信息认证码;

A2:根据消息载荷长度配置,对信息认证码进行截取;

A3:将原始数据、信息认证码、计数器值连接组成认证数据;

A4:使用加密算法加密认证数据,获取加密数据;

A5:广播发送加密数据,传输启动后将计数器值加1。

3.根据权利要求1所述的一种商用车远程防盗系统,其特征在于,所述解密机制具体如下:

B1:使用解密算法解密接收到的加密数据,获得待认证数据;

B2:从待认证数据中解析出原始数据、信息认证码、计数器值;

B3:将新收到的计数器值与上次存储的计数器值进行比较,若不大于存储的计数器值则停止校验,丢弃此数据;若大于存储的计数器值则完成校验,并存储新的计数器值;

B4:通过校验后,将拼接了计数器值的原始数据和密钥作为认证算法输入,计算获取信息认证码,并与B2解析到的消息认证码进行对比,完成认证工作;

B5:通过认证后,完成原始数据的解密。

4.根据权利要求1所述的一种商用车远程防盗系统,其特征在于,所述加密/解密算法采用XXTEA算法,所述认证算法采用HMAC算法。

5.根据权利要求1所述的一种商用车远程防盗系统,其特征在于,所述控制主机连接挂

车车锁，用于解锁或上锁挂车车锁；所述控制主机连接车用轮速传感器和报警提示灯，在执行上锁工作时，车用轮速传感器获取车辆行驶速度，当驾驶速度不为零时，通过报警提示灯提示司机降速。

6.根据权利要求1所述的一种商用车远程防盗系统，其特征在于，所述远程信息处理终端采用车规级微控制器芯片，连接通信模组，支持采集信号内容可配置，信号解析方式可配置，CAN总线频率可配置。

7.根据权利要求1所述的一种商用车远程防盗系统，其特征在于，所述远程信息管理平台包括后台、中台和前台；

所述后台包括数据库和传输协议解析层；

所述数据库包括MongoDB、MySQL、InfluxDB，用于保存不同类型的数据，所述传输协议解析层用于实现数据接收、解析和分发工作；

所述中台包括消息中间件和消息缓存；

所述消息中间件用于实现前台和后台间的数据交换，所述消息缓存用于保存最近的数据信息，实现前台的快速查询；

所述前台用于数据查询与可视化、下发控制命令和更新授权信息等功能。

8.根据权利要求1所述的一种商用车远程防盗系统，其特征在于，所述数据输入模块和所述控制主机以及所述控制主机和所述远程信息处理终端通过CAN总线进行数据交互，并按照国家标注J1939规定的数据传输格式进行传输；所述远程信息处理终端与所述远程信息管理平台按照国家标准JT/T808规定的数据传输格式进行传输，标准未规定的信号采用自定义的信号ID进行传输，传输数据支持加密和非加密。

9.一种权利要求1至8任一项所述的商用车远程防盗系统的工作方法，其特征在于，包括信息预置、解锁和上锁三个部分；

所述信息预置包括两种方式：

T1本地信息预置：车头连接外置诊断盒，输入管理员密码，可修改控制主机预置的授权信息；

T2云端信息更新：管理员使用管理员账号登陆远程信息管理平台，针对某辆商用车在平台上修改授权信息，将信息传输至远程信息处理终端，通过其存储模块进行存储，当接收到控制主机的授权信息更新请求时，下发到控制主机进行预置信息更新；

所述解锁方法包括以下步骤：

S1：授权信息提前以短信形式发送到司机手机；

S2：司机使用身份卡在数据输入模块进行刷卡操作，身份识别器读取司机身份卡信息，附属控制器将身份信息加密后传输到控制主机；

S3：控制主机进行解密得到司机身份卡信息，与控制主机预置的授权信息进行匹配验证，若验证通过则执行解锁工作，若验证失败控制主机将提醒司机，并向远程信息管理平台发送尝试解锁标志，远程信息管理平台会以短信方式告知未正常解锁原因；

所述上锁方法包括两种方式：

L1立即上锁：远程信息管理平台下发立即上锁命令，远程信息处理终端接收上锁命令并转发给控制主机，控制主机接收到上锁命令会根据当前车速向司机发送停车提醒；

L2时间段上锁：远程信息管理平台可以设置授权时间段，在时间段内车辆可以进行解

锁,超过授权时间段,司机不再有权限解锁挂车。

10.根据权利要求9所述的方法,其特征在于,基于授权时间段进行管理,具体为:

L21:远程信息管理平台下发最新的授权时间段到远程信息处理终端并进行存储;

L22:每次上电时,控制主机向远程信息处理终端发送授权信息更新请求,远程信息处理终端接收控制主机发送的授权信息更新请求后,将授权时间段加密后发送至控制主机,并存储在控制主机;

L23:控制主机每次进行解锁时,读取其存储的授权时间段信息,判断是否有权限解锁;临近授权时间段到期,控制主机执行上锁工作。

商用车远程防盗系统及其工作方法

技术领域

[0001] 本发明涉及汽车防盗领域，具体涉及一种商用车远程防盗系统以及防盗系统工作方法。

背景技术

[0002] 物流行业的快速发展给商用车带来了新的运营模式，以往，商用车驾驶员自己管理车头及挂车，运输也独立完成。但随着商用车驾驶员运输效率和行业需求的不匹配，物流公司应运而生。物流公司拥有数量庞大的车队(挂车)，驾驶员在物流公司分配任务后使用自己的车头连接物流公司的挂车来完成一次出车任务。区别以往车头和挂车一对一的使用模式，多对多的使用模式会带来更多安全性问题，包括：非授权驾驶员控制挂车、驾驶员控制挂车超过授权时间、驾驶员解锁信息被盗等等。因此，需要设计一套商用车智能防盗系统。

[0003] 随着云技术发展，更多的管理工作可以依托云平台来实现。平台可以帮助企业管理所有数据，在这些数据基础上可以进行拓展任务的开发。同时，平台可以轻松设置不同级别的权限，确保在适当的时间有合适的人员安全地访问正确的信息。因此，基于云平台的商用车远程防盗系统具有重要意义。

发明内容

[0004] 本发明的目的在于针对上述行业需求，提出一种商用车远程防盗系统及防盗系统工作方法，基于驾驶员身份卡信息解锁，添加加密解密模块进行信息传输，使用远程信息管理平台来完成商用车的防盗及管理任务。

[0005] 为达到上述目的，本发明是通过以下技术方案实现的：

[0006] 本发明一方面提供了一种商用车远程防盗系统，包括数据输入模块、控制主机、远程信息处理终端和远程信息管理平台；

[0007] 所述数据输入模块包括身份识别器和附属控制器，所述身份识别器用于识别司机专属身份卡信息，所述附属控制器用于将司机身份卡信息加密后传输至控制主机；

[0008] 所述控制主机包括存储模块和解密模块，接收所述数据输入模块传输来的信息，通过解密模块对信息进行解密得到司机身份卡信息，与存储模块中预置的授权信息进行匹配验证，授权信息包括有效司机身份卡信息和授权时间段，验证通过后执行解锁工作，并将商用车当前上锁/解锁状态传输至远程信息处理终端；接收所述远程信息处理终端传输的控制指令，执行相应的解锁/上锁工作，并将商用车当前上锁/解锁状态传输至远程信息处理终端；在上电时，向远程信息处理终端发送授权信息更新请求，接收远程信息处理终端传输的最新授权信息，通过解密模块进行解密得到最新的有效司机身份卡信息和授权时间段，更新存储模块中预置授权信息；

[0009] 所述远程信息处理终端包括存储模块和加密模块，用于将所述控制主机传输的商用车当前上锁/解锁状态转发至远程信息管理平台；将远程信息管理平台下发的控制指令

转发至控制主机，将远程信息管理平台下发的授权信息存储在其存储模块；接收控制主机发送的授权信息更新请求后，将存储模块中的授权信息通过加密模块加密后发送至控制主机；

[0010] 所述远程信息管理平台用于可视化当前商用车状态以及司机的信息，管理员可通过所述远程信息管理平台下发上锁/解锁控制指令及更新授权信息。

[0011] 进一步地，所述加密机制具体如下：

[0012] A1：将拼接了计数器值的原始数据和密钥作为认证算法的输入，计算获取信息认证码；

[0013] A2：根据消息载荷长度配置，对信息认证码进行截取；

[0014] A3：将原始数据、信息认证码、计数器值连接组成认证数据；

[0015] A4：使用加密算法加密认证数据，获取加密数据；

[0016] A5：广播发送加密数据，传输启动后将计数器值加1。

[0017] 进一步地，所述解密机制具体如下：

[0018] B1：使用解密算法解密接收到的加密数据，获得待认证数据；

[0019] B2：从待认证数据中解析出原始数据、信息认证码、计数器值；

[0020] B3：将新收到的计数器值与上次存储的计数器值进行比较，若不大于存储的计数器值则停止校验，丢弃此数据；若大于存储的计数器值则完成校验，并存储新的计数器值；

[0021] B4：通过校验后，将拼接了计数器值的原始数据和密钥作为认证算法的输入，计算获取信息认证码，并与B2解析到的消息认证码进行对比，完成认证工作；

[0022] B5：通过认证后，完成原始数据的解密。

[0023] 进一步地，所述加密/解密算法使用的是XXTEA算法，所述的认证算法使用的是HMAC算法。

[0024] 进一步地，所述控制主机连接挂车车锁，用于解锁或上锁挂车车锁；所述控制主机连接车用轮速传感器和报警提示灯，在执行上锁工作时，车用轮速传感器获取车辆行驶速度，当驾驶速度不为零时，通过报警提示灯提示司机降速。

[0025] 进一步地，所述远程信息处理终端采用车规级微控制器芯片，连接通信模组，支持采集信号内容可配置，信号解析方式可配置，CAN总线频率可配置。

[0026] 进一步地，所述远程信息管理平台包括后台、中台和前台；

[0027] 所述后台包括数据库和传输协议解析层；

[0028] 所述数据库包括MongoDB、MySQL、InfluxDB，用于保存不同类型的数据，所述传输协议解析层用于实现数据接收、解析和分发工作；

[0029] 所述中台包括消息中间件和消息缓存；

[0030] 所述消息中间件用于实现前台和后台间的数据交换，所述消息缓存用于保存最近的数据信息，实现前台的快速查询；

[0031] 所述前台用于数据查询与可视化、下发控制命令和更新授权信息等功能。

[0032] 进一步地，所述数据输入模块和所述控制主机以及所述控制主机和所述远程信息处理终端通过CAN总线进行数据交互，并按照国家标注J1939规定的数据传输格式进行传输。

[0033] 进一步地，所述远程信息处理终端与所述远程信息管理平台按照国家标准JT/

T808规定的数据传输格式进行传输，标准未规定的信号采用自定义的信号ID进行传输，传输数据支持加密和非加密。

[0034] 本发明另一方面提供了一种商用车远程防盗系统的工作方法，包括信息预置、解锁和上锁三个部分：

[0035] 所述信息预置包括两种方式：

[0036] T1本地信息预置：车头连接外置诊断盒，输入管理员密码，可修改控制主机预置的授权信息；

[0037] T2云端信息更新：管理员使用管理员账号登陆远程信息管理平台，针对某辆商用车在平台上修改授权信息，将信息传输至远程信息处理终端，通过其存储模块进行存储，当接收到控制主机的授权信息更新请求时，下发到控制主机进行预置信息更新。

[0038] 所述解锁方法包括以下步骤：

[0039] S1：授权信息提前以短信形式发送到司机手机；

[0040] S2：司机使用身份卡在数据输入模块进行刷卡操作，身份识别器读取司机身份卡信息，附属控制器将身份信息加密后传输到控制主机；

[0041] S3：控制主机进行解密得到司机身份卡信息，与控制主机预置的授权信息进行匹配验证，若验证通过则执行解锁工作，若验证失败控制主机将提醒司机，并向远程信息管理平台发送尝试解锁标志，远程信息管理平台会以短信方式告知未正常解锁原因。

[0042] 所述上锁方法包括两种方式：

[0043] L1立即上锁：远程信息管理平台下发立即上锁命令，远程信息处理终端接收上锁命令并转发给控制主机，控制主机接收到上锁命令会根据当前车速向司机发送停车提醒；

[0044] L2时间段上锁：远程信息管理平台可以设置授权时间段，在时间段内车辆可以进行解锁，超过授权时间段，司机不再有权限解锁挂车。

[0045] 进一步地，所述商用车远程防盗系统基于授权时间段进行管理，包括：

[0046] L21：远程信息管理平台下发最新的授权时间段到远程信息处理终端并进行存储；

[0047] L22：每次上电时，控制主机向远程信息处理终端发送授权信息更新请求，远程信息处理终端接收控制主机发送的授权信息更新请求后，将授权时间段加密后发送至控制主机，并存储在控制主机；

[0048] L23：控制主机每次进行解锁时，读取其存储的授权时间段信息，判断是否有权限解锁；临近授权时间段到期，控制主机执行上锁工作。

[0049] 本发明的有益效果是：本发明设计了一种商用车远程防盗系统及其工作方法，针对CAN通信时信息泄漏、数据被修改、受到重放攻击等问题，本发明在传统的CAN数据传输上增加加密/解密机制，通过向原始数据中融入计数器值和消息认证码并共同进行加解密操作来实现；本发明在网络良好状态下将授权信息实时下发到远程信息处理终端进行存储，每次上电后控制主机直接向远程信息处理终端请求更新授权信息，更新操作基于本地CAN通信实现无需使用蜂窝无线网络，防止因网络问题导致信息预置失败影响系统工作；本发明还基于远程信息管理平台对挂车和驾驶员信息可视化管理，并实现下发解锁上锁控制命令和更新授权信息的功能，从而帮助物流公司实现远程车队管理及挂车防盗工作。

附图说明

[0050] 图1为本发明实施例提供的商用车远程防盗系统的结构框图；

[0051] 图2为本发明实施例提供的数据加密流程；

[0052] 图3为本发明实施例提供的数据解密流程；

[0053] 图4为本发明实施例提供的解锁方法流程图；

[0054] 图5为本发明实施例提供的基于授权时间段管理方法流程图。

具体实施方式

[0055] 为了更好的理解本申请的技术方案，下面结合附图对本申请实施例进行详细描述。

[0056] 应当明确，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其它实施例，都属于本申请保护的范围。

[0057] 在本申请实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。

[0058] 图1为本发明实施例提供的商用车远程防盗系统的结构框图，如图1所示，该系统包括数据输入模块101、控制主机102、远程信息处理终端103和远程信息管理平台104。

[0059] 具体地，数据输入模块101包括身份识别器和附属控制器，身份识别器用于识别司机专属身份卡信息，附属控制器用于将司机身份卡信息加密后传输至控制主机；本系统的解锁方式采用司机身份卡，数据输入模块将完成司机身份卡读取、加密以及传输工作。

[0060] 具体地，控制主机102包括存储模块和解密模块，接收数据输入模块传输来的信息，通过解密模块对信息进行解密得到司机身份卡信息，与存储模块中预置的授权信息进行匹配验证，授权信息包括有效司机身份卡信息和授权时间段，验证通过后执行解锁工作，并将商用车当前上锁/解锁状态传输至远程信息处理终端；接收远程信息处理终端传输的控制指令，执行相应的解锁/上锁工作，并将商用车当前上锁/解锁状态传输至远程信息处理终端；在上电时，向远程信息处理终端发送授权信息更新请求，接收远程信息处理终端传输的最新授权信息，通过解密模块进行解密得到最新的有效司机身份卡信息和授权时间段，更新存储模块中预置授权信息。

[0061] 具体地，控制主机还连接挂车车锁，用于解锁或上锁挂车车锁；控制主机还连接车用轮速传感器和报警提示灯，在执行上锁工作时，车用轮速传感器获取车辆行驶速度，当驾驶速度不为零时，通过报警提示灯提示司机降速。

[0062] 具体地，远程信息处理终端103包括存储模块和加密模块，用于将控制主机传输的商用车当前上锁/解锁状态转发至远程信息管理平台；将远程信息管理平台下发的控制指令转发至控制主机，将远程信息管理平台下发的授权信息存储在其存储模块；接收控制主机发送的授权信息更新请求后，将存储模块中的授权信息通过加密模块加密后发送至控制主机。

[0063] 具体地，远程信息处理终端采用车规级微控制器芯片，连接通信模组，支持采集信号内容可配置，信号解析方式可配置，CAN总线频率可配置。

[0064] 具体地，远程信息管理平台104用于可视化当前商用车状态以及司机的信息，管理员可通过所述远程信息管理平台下发上锁/解锁控制指令及更新授权信息；远程信息管理平台包括后台、中台、前台：

[0065] 这里后台包括数据库和808交通标准传感接入层，数据库包括MongoDB、MySQL、InfluxDB，用于保存不同类型的数据，808交通标准传感接入层用于实现数据接收、解析和分发工；

[0066] 这里中台包括消息中间件和消息缓存，消息中间件用于实现前台和后台间的数据交换，消息缓存用于保存最近的数据信息，实现前台的快速查询；

[0067] 这里前台用于数据查询与可视化、下发控制命令和更新授权信息等功能。

[0068] 具体地，数据输入模块和控制主机以及控制主机和远程信息处理终端通过CAN总线进行数据交互，并按照国家标注J1939规定的数据传输格式进行传输。

[0069] 具体地，远程信息处理终端与远程信息管理平台按照国家标准JT/T808规定的数据传输格式进行传输，标准未规定的信号采用自定义的信号ID进行传输，传输数据支持加密和非加密。

[0070] 图2和图3是数据输入模块和控制主机以及控制主机和远程信息处理终端CAN通信时数据的加密解密流程。

[0071] 具体地，使用的加密机制如下：

[0072] 201：控制每条原始数据在48位以内，不足补齐48位，初始化一个计数器值，用6位表示，将原始数据、密钥K1、计数器值作为认证算法的输入，此处使用HMAC算法计算信息认证码；

[0073] 202：根据消息载荷长度配置，对信息认证码进行截取，考虑到CAN数据只有8个字节有效载荷，所以一般截取10位最高有效位；

[0074] 203：将原始数据、信息认证码、计数器值连接组成8个字节的认证数据；

[0075] 204：使用加密算法加密认证数据，获取加密数据，此处使用XXTEA加密算法；

[0076] 205：广播发送加密数据，传输启动后将计数器值加1。

[0077] 具体地，使用的解密机制如下：

[0078] 301：使用解密算法解密接收到的加密数据，这里使用XXTEA解密算法，获得待认证数据；

[0079] 302：从待认证数据中解析出原始数据(48位)、信息认证码(10位)、计数器值(6位)；

[0080] 303：将新收到的计算器值与上次存储的计算器值进行比较，若不大于存储的计数器值则停止校验，丢弃此数据；若大于存储的计算器值则完成校验，并存储新的计数器值；

[0081] 304：通过校验后，将拼接了计数器值的原始数据和密钥作为认证算法的输入，计算获取信息认证码，并与步骤302解析到的消息认证码进行对比，如果相同则通过认证，不相同则停止认证，丢弃此数据；

[0082] 305：通过认证后，完成原始数据的解密，将原始数据传送到应用层进行后续的功能判断。

[0083] 本发明还提供了一种上述商用车远程防盗系统的工作方法，包括信息预置、解锁和上锁三个部分。

[0084] 具体地，信息预置方法包括两种方式：

[0085] 本地信息预置：车头连接外置诊断盒，输入管理员密码，可修改控制主机预置的授权信息；

[0086] 云端信息更新：管理员使用管理员账号登陆远程信息管理平台，针对某辆商用车在平台上修改授权信息，将信息传输至远程信息处理终端，通过其存储模块进行存储，当接收到控制主机的授权信息更新请求时，下发到控制主机进行预置信息更新。

[0087] 具体地，图4为解锁方法的流程图，包括以下步骤：

[0088] 401：授权信息提前以短信形式发送到司机手机；

[0089] 402：司机使用身份卡在数据输入模块进行刷卡操作，身份识别器读取司机身份卡信息，附属控制器将身份信息加密后传输到控制主机；

[0090] 403：控制主机进行解密得到司机身份卡信息，与控制主机预置的授权信息进行匹配验证，若验证通过则执行解锁工作，若验证失败控制主机将提醒司机，并向远程信息管理平台发送尝试解锁标志，远程信息管理平台会以短信方式告知未正常解锁原因。

[0091] 具体地，上锁方法包括两种方式：

[0092] 立即上锁：远程信息管理平台下发立即上锁命令，远程信息处理终端接收上锁命令并转发给控制主机，控制主机接收到上锁命令会根据当前车速向司机发送停车提醒；

[0093] 时间段上锁：远程信息管理平台可以设置授权时间段，在时间段内车辆可以进行解锁，超过授权时间段，司机不再有权限解锁挂车。

[0094] 图5是基于授权时间段管理方法的流程图，包括以下步骤：

[0095] 501：远程信息管理平台下发最新的授权时间段到远程信息处理终端并进行存储；

[0096] 502：每次上电时，控制主机向远程信息处理终端发送授权信息更新请求，远程信息处理终端接收控制主机发送的授权信息更新请求后，将授权时间段加密后发送至控制主机，并存储在控制主机；

[0097] 503：控制主机每次进行解锁时，读取其存储的授权时间段信息，判断是否有权限解锁；临近授权时间段到期，控制主机执行上锁工作。

[0098] 综上所述，本发明提出的商用车远程防盗系统及其工作方法，针对CAN通信时信息泄漏、数据被修改、受到重放攻击等问题，本发明在传统的CAN数据传输上增加加密/解密机制，通过向原始数据中融入计数器值和消息认证码并共同进行加解密操作来实现；本发明在网络良好状态下将授权信息实时下发到远程信息处理终端进行存储，每次上电后控制主机直接向远程信息处理终端请求更新授权信息，更新操作基于本地CAN通信实现无需使用蜂窝无线网络，防止因网络问题导致信息预置失败影响系统工作；本发明还基于远程信息管理平台对挂车和驾驶员信息可视化管理，并实现下发解锁/上锁控制命令和更新授权信息的功能，从而帮助物流公司实现远程车队管理及挂车防盗工作。本发明充分利用现有的身份识别器功能，在此基础上增加防盗功能的系统化设计，易于在实际商用车上实现和运行。

[0099] 以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围，凡在本发明的精神和原则之内所做的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

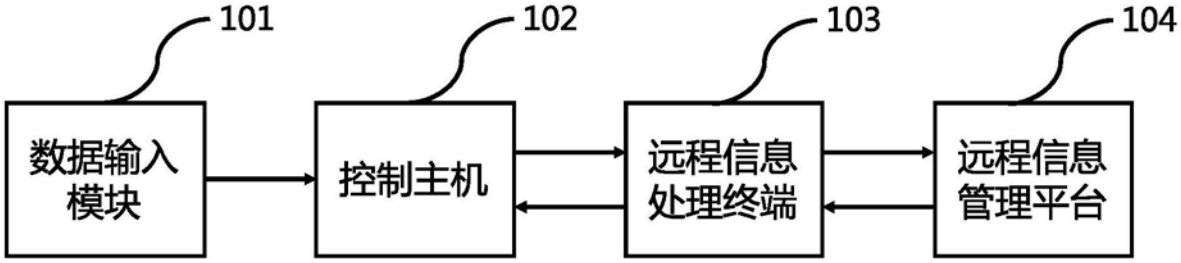

101
102
103
104
数据输入模块
控制主机
远程信息处理终端
远程信息管理平台

图1

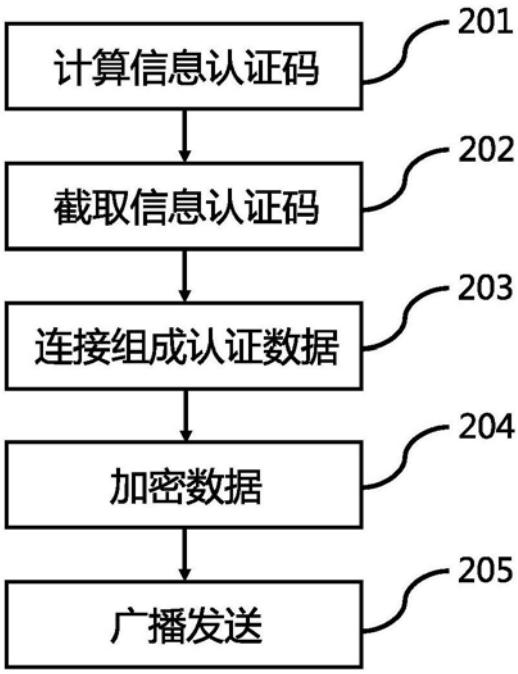

201
计算信息认证码
202
截取信息认证码
203
连接组成认证数据
204
加密数据
205
广播发送

图2

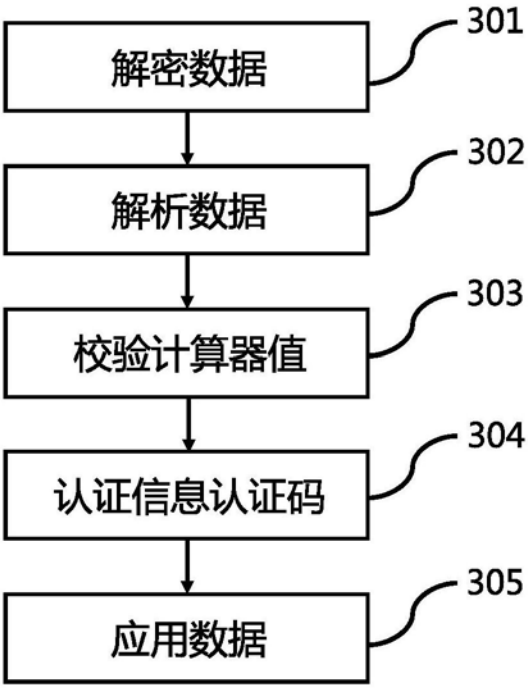

解密数据
301
解析数据
302
校验计算器值
303
认证信息认证码
304
应用数据
305

图3

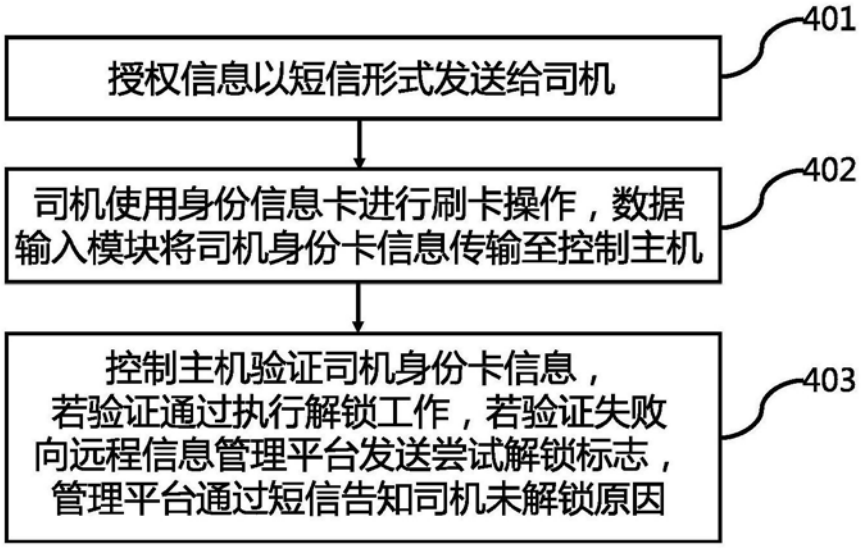

授权信息以短信形式发送给司机
401
司机使用身份信息卡进行刷卡操作，数据输入模块将司机身份卡信息传输至控制主机
402
控制主机验证司机身份卡信息，若验证通过执行解锁工作，若验证失败向远程信息管理平台发送尝试解锁标志，管理平台通过短信告知司机未解锁原因
403

图4

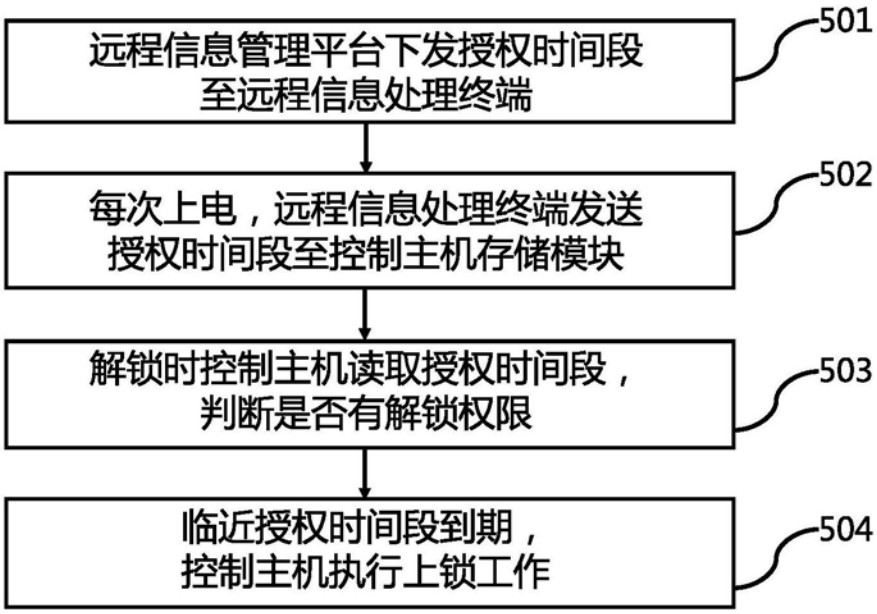

远程信息管理平台下发授权时间段
至远程信息处理终端
501
每次上电，远程信息处理终端发送
授权时间段至控制主机存储模块
502
解锁时控制主机读取授权时间段，
判断是否有解锁权限
503
临近授权时间段到期，
控制主机执行上锁工作
504

图5